Remarks

Status of application

Claims 1-55 were examined and stand rejected in view of prior art. The claims have been amended to further clarify Applicant's invention. Reexamination and reconsideration are respectfully requested.

General

A minor amendment to the specification has been entered to correct an informality introduced by the Office's PTO Electronic Stylesheet v. 1.1.1 (which was required, pursuant to electronic filing).

The invention

A system providing a secure lockbox methodology for protecting sensitive information is described. In one embodiment, the methodology includes steps of receiving input of sensitive information from a user; computing a data shadow of the sensitive information for storage in a repository; based on the data shadow stored in the repository, detecting any attempt to transmit the sensitive information; and blocking any detected attempt to transmit the sensitive information that is not authorized (e.g., by the user).

Prior art rejections

A. Rejection under 35 U.S.C. 102(e): Margolus

Claims 1-55 stand rejected under 35 U.S.C. 102(e) as being anticipated by Margolus et al. in US Patent Application Publication No. 2004/0162808 (hereinafter, "Margolus"). Here, the Examiner likens Applicant's invention to Margolus' data repository that promotes network storage of data.

At the outset, it is important to understand that Applicant does not claim to have invented the notion of computing a fingerprint on data. For example, as Margolus aptly points out (e.g., Margolus at [0006]), the concept of a "digital fingerprint" of a file, also called a "hash function", a "content signature" or a "message digest", is well known. Margolus explains, at [0007], that fingerprints have been used for many years to avoid

unnecessary file transfers. One application of this sort has been in Bulletin Board Systems (BBSs), which have used fingerprints since the early 1990's to avoid the communication cost of uploading file data that is already present in the BBS, but associated with a different file name. A client computer wishing to store data into the BBS can compute the fingerprint of the file that it wishes to send, and send that first. If a file containing this data is already present in the BBS, then the client is informed and need not send anything. The scheme uses fingerprints to identify redundant data and avoid unnecessary transmission and storage.

With the above basic notion of a digital fingerprint, Margolus describes an approach for promoting network storage of data. Margolus describes a method by which more than one client program connected to a network stores the same data item on a storage device of a data repository connected to the network. The method comprises encrypting the data item using a key derived from the content of the data item, determining a digital fingerprint of the data item, and **storing the data item on the storage device** at a location or locations associated with the digital fingerprint. Importantly, as indicated by the foregoing highlights, Margolus' approach is one in which the data item is required to be stored. That approach is essentially the antithesis of Applicant's approach, as will now be described in detail.

A core feature of Applicant's invention is that the **data item** of interest (e.g., sensitive information) **is itself not stored**. Consider the following from Applicant's Background Section (describing the problems of the prior art):

> Another solution that solves much of this growing problem involves running a software agent to monitor the PC's network traffic. This simplified or basic "lockbox" approach ensures that sensitive information is not transmitted outside the local host without the user's knowledge. If sensitive information is discovered during this process, the underlying security engine may give the user the ability to block or modify the outgoing request. [...]
>
> The simplified lockbox approach has its problems, however. **Storage of reference copies of the sensitive information in a simple**

lockbox creates a new point of vulnerability. The lockbox itself becomes a potential target for attack and compromise. Therefore, a better solution is sought.

(Applicant's Specification, at [0011] - [0012])

Importantly, in order to avoid the above-identified vulnerability (as described in Applicant's Background Section), the data item itself is not stored at all in Applicant's system.

How is it possible to have a system that does not store the data item? Note particularly that the data item of interest to Applicant's invention typically comprises "input of sensitive information from a user" (see, e.g., Applicant's claim 1), such as a Social Security number, a password, or the like. In accordance with Applicant's invention, therefore, this sensitive information is not stored since, if it were stored, then it may serve as a point of vulnerability (i.e., subject to attack and compromise by hackers, etc.). Instead, a data "shadow" is created so that the original input of the sensitive information may in fact be discarded. Therefore, not only is the sensitive information not stored in Applicant's system, but also the data shadow is created for the express purpose of allowing the original data item (input of sensitive information) to be discarded. By discarding the data item (e.g., Social Security number, password, etc.), that data item no longer remains as vulnerable data present on the user's system. No matter how hard a hacker tries, he or she will be unable to retrieve a copy of the sensitive information from the user's system, as no copy in fact exists. Further, the hacker will be unable to reconstitute the sensitive information from the data shadow, as the data shadow itself is a cryptographically secured hash (e.g., MD-5), which makes reconstitution of the original sensitive information computationally infeasible.

Although Applicant's originally filed claims are believed to distinguish over the cited art, the claims have nevertheless been amended in an effort to further clarify Applicant's claimed invention and expedite prosecution of the present application. For example, independent claim 1 has been amended to include the claim limitation of (shown in amended form):

computing a data shadow of the sensitive information for storage in a repository, and thereafter discarding the input so that the sensitive information itself is not stored;

(Applicant's other independent claims were amended in a like manner.) The foregoing amendment to the claim makes it explicitly clear that the sensitive information itself is in fact discarded after computation of the data shadow. The sensitive information itself is **not stored** at all, as part of the process. In fact, if the sensitive information were stored, that would defeat the purpose of Applicant's invention. The primary purpose and utility of Applicant's invention is an improved lockbox that stores data "shadows," so that the underlying sensitive information itself **need not be stored** on the subject computer. In this manner, the data shadows can detect an attempted transmission of sensitive information, even though a copy of the sensitive information itself is not and was not stored on the subject computer.

All told, Applicant's data shadow approach (which expressly eschews storage of the data item itself) is not taught or suggested by Margolus' network storage solution. As Margolus' approach is in fact one "promoting" the storage of a data item itself on network storage, the Margolus' approach teaches if anything away from Applicant's data shadow approach. In view of the foregoing amendments and clarifying remarks made above, it is respectfully submitted that the claims set forth a patentable advance over the art, and that any rejection under Section 102(e) is overcome.

Any dependent claims not explicitly discussed are believed to be allowable by virtue of dependency from Applicant's independent claims, as discussed in detail above.

Conclusion

In view of the foregoing remarks and the amendment to the claims, it is believed that all claims are now in condition for allowance. Hence, it is respectfully requested that the application be passed to issue at an early date.

If for any reason the Examiner feels that a telephone conference would in any way expedite prosecution of the subject application, the Examiner is invited to telephone the undersigned at 408 884 1507.

Respectfully submitted,

Date: March 12, 2007

/John A. Smart/

John A. Smart; Reg. No. 34,929
Attorney of Record

408 884 1507
815 572 8299 FAX